



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,301	10/09/2001	Philip Hawkes	020002	6013
23696	7590	11/29/2005	EXAMINER	
QUALCOMM, INC 5775 MOREHOUSE DR. SAN DIEGO, CA 92121			CERVETTI, DAVID GARCIA	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	09/973,301		HAWKES ET AL.	
	Examiner		Art Unit	
	David G. Cervetti		2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 September 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's arguments filed September 6, 2005, have been fully considered but they are not persuasive.
2. Claims 1-24 are pending and have been examined.

Response to Amendment

3. The objection to the drawings is withdrawn.
4. The objection to claim 6 is withdrawn.
5. Pierce et al. (US Patent Number 5,467,398, hereinafter "Pierce") teaches the messaging key associated with a reference number (a short term key and a key identifier), transmitting information in the Internet (it is conventional and well known that when information is transmitted in the Internet, internet protocol headers are prepared and sent. Assuming Applicant is correct on the interpretation of the prior art references, and the prior art does not, alone or in combination, teach, suggests, or otherwise motivates, someone of ordinary skill in the art to use the conventional and well known short term keys, the prior art of record, namely Menezes et al. (NPL "Handbook of Applied Cryptography", hereinafter "Menezes"), teaches using short term keys (session keys), master keys, key encrypting keys, and data keys (page 551-552 and remaining of chapter 13). Therefore, assuming *arguendo* that Pierce does not teach or suggests the claimed invention, but agreeing that he at the very least gives the architecture needed for the invention, applying the teachings of Menezes to the system of Pierce would have been obvious to one of ordinary skill in the art.

Claim Objections

6. Claim 7 is objected to because of the following informalities: "ESP" must be spelled out. Appropriate correction is required.

Claim Rejections - 35 USC § 101

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 21-24 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 21 states "an infrastructure element for a wireless communication system (apparatus), comprising: means for receiving, determining, encrypting, and decrypting". These limitations are considered non-statutory subject matter because they consist on software code for receiving, determining, encrypting, and decrypting (page 3, paragraph [1007]). The claims are not limited to tangible embodiments. Applicant has invoked USC 112, 6th paragraph by using "means plus function language". In view of page 3, paragraph 1007 of the specification which describes that each of the means may be software, the fact that they may also be embodied in hardware is not persuasive.

Claim 22 states "a digital signal storage device", a digital signal is considered non-statutory subject matter. Furthermore, the limitations are considered non-statutory subject matter because they consist on software code for receiving a short term key identifier, determining an access key based on the short term key identifier, encrypting the short term key identifier with the access key to recover the short term key, and decrypting the transmission using the short term key. A digital signal does not fall within

Art Unit: 2136

the categories of patentable subject matter set forth in USC 101. The fact that the signal is stored, is not persuasive.

Claim 23 states “a storage device having stored a communication signal transmitted on a carrier wave”; a “communication signal transmitted on a carrier wave” is considered non-statutory subject matter. Furthermore, the communication signal claimed comprises two portions, a key identifier and an encrypted payload. Considering a data structure to be “a physical or logical relationship among data elements, designed to support specific data manipulation functions” (IEEE Standard Dictionary of Electrical and Electronic Terms 308, 5th edition, 1993), this is considered non-functional descriptive material that does not constitute a statutory process, machine, manufacture, or composition of matter.

Claim 24 is rejected based on its dependency from claim 23.

9. To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1-6 and 14-24 are rejected under 35 U.S.C. 102(b) as being anticipated by Pierce.

Regarding claim 1, Pierce teaches

determining a short term key for a message for transmission, the short term key having a short term key identifier (column 2, lines 44-47);

determining an access key for the message, the access key having an access key identifier (column 2, lines 47-50);

encrypting the message with the access key (column 2, lines 50-52);

forming an Internet protocol header comprising the short term key identifier (column 2, lines 52-53); and

transmitting the encrypted message with the Internet protocol header (column 2, lines 52-55).

Regarding claim 2, Pierce teaches wherein the short term key identifier comprises the access key identifier (column 2, lines 40-58).

Regarding claim 3, Pierce teaches wherein short term key identifier further comprises a security parameter index value (column 2, lines 40-58).

Regarding claim 4, Pierce teaches wherein the security parameter index value is a random number (column 2, lines 40-58, column 4, lines 55-65).

Regarding claim 5, Pierce teaches wherein the short term key is calculated as a function of the short term key identifier and the access key (column 2, lines 40-58, column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 6, Pierce teaches wherein the short term key is calculated by encrypting the short term key identifier with the access key (column 2, lines 40-58, column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 14, Pierce teaches receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key (column 4, lines 5-10);

determining an access key based on the short term key identifier (column 4, lines 7-13);

encrypting the short term key identifier with the access key to recover the short term key (column 4, lines 13-16); and

decrypting the transmission using the short term key (column 4, lines 25-30).

Regarding claim 15, Pierce teaches storing the short term key identifier and short term key in a memory storage unit (figure 1, reference character 111, 105, column 4, lines 5-55).

Regarding claim 16, Pierce teaches wherein the short term key identifier is comprised of a random number and an access key identifier associated with the access key (column 4, lines 5-55, column 5, lines 1-25).

Regarding claim 17, Pierce teaches wherein encrypting the short term key identifier further comprises encrypting the short term key identifier and a random

Art Unit: 2136

number with the access key to recover the short term key (column 4, lines 5-67, column 5, lines 1-25).

Regarding claim 18, Pierce teaches

a receive circuitry (column 4, lines 5-10);

a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising:

processing unit operative to decrypt key information (column 4, lines 25-30); and

a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message, comprising:

memory storage unit for storing a plurality of short term keys and short term key identifiers (column 3, lines 26-67, column 4, lines 1-67).

Regarding claim 19, Pierce teaches wherein the user identification unit further comprises a second memory storage unit for storing a plurality of access keys and access key identifiers (column 4, lines 35-55).

Regarding claim 20, Pierce teaches wherein the memory storage unit is a secure memory storage unit (column 4, lines 35-55).

Regarding claim 21, Pierce teaches

means for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key;

means for determining an access key based on the short term key identifier;

means for encrypting the short term key identifier with the access key to recover the short term key; and

Art Unit: 2136

means for decrypting the transmission using the short term key (column 3, lines 53-67, column 4, lines 1-35).

Regarding claim 22, Pierce teaches

first set of instructions for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key (column 3, lines 53-67, column 4, lines 1-5);

second set of instructions for determining an access key based on the short term key identifier (column 4, lines 5-25);

third set of instructions for encrypting the short term key identifier with the access key to recover the short term key (column 4, lines 5-25); and

fourth set of instructions for decrypting the transmission using the short term key (column 4, lines 25-35).

Regarding claim 23, Pierce teaches

a first portion corresponding to a short term key identifier, the short term key identifier having a corresponding short term key; and

a second portion corresponding to a transmission payload encrypted using the short term key (column 4, lines 55-67, column 5, lines 1-50).

Regarding claim 24, Pierce teaches

wherein the short term key identifier comprises:

a random number portion; and

an access key identifier corresponding to an access key (column 4, lines 55-65).

Claim Rejections - 35 USC § 103

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pierce, and further in view of Nessett et al. (US Patent Number 6,055,236, hereinafter "Nessett").

Regarding claim 7, Pierce does not disclose expressly wherein the Internet protocol header is part of an ESP header. However, Nessett teaches wherein the Internet protocol header is part of an ESP header (column 21, lines 53-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use Encapsulating Security Payload with the Internet Protocol. One of ordinary skill in the art would have been motivated to do so because ESP provides encryption protection and optional authentication and integrity protection (Nessett, column 21, lines 1-67, column 22, lines 1-67).

Regarding claim 8, the combination of Pierce and Nessett teaches the limitations as set forth under claim 7 above. Furthermore, Pierce teaches wherein the Internet protocol header further comprises a second random number, the second random number having a random number identifier (column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 9, the combination of Pierce and Nessett teaches the limitations as set forth under claim 8 above. Furthermore, Pierce teaches wherein the

Art Unit: 2136

short term key identifier comprises the access key identifier and the random number identifier (column 2, lines 40-58, column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 10, the combination of Pierce and Nessett teaches the limitations as set forth under claim 9 above. Furthermore, Pierce teaches wherein short term key identifier further comprises a security parameter index value (column 4, lines 35-55).

Regarding claim 11, the combination of Pierce and Nessett teaches the limitations as set forth under claim 10 above. Furthermore, Pierce teaches wherein the security parameter index value is a random number (column 4, lines 35-67, column 5, lines 1-25).

Regarding claim 12, the combination of Pierce and Nessett teaches the limitations as set forth under claim 8 above. Furthermore, Pierce teaches wherein the short term key is calculated as a function of the short term key identifier, the second random number, and the access key (column 4, lines 5-67, column 5, lines 1-25).

Regarding claim 13, the combination of Pierce and Nessett teaches the limitations as set forth under claim 12 above. Furthermore, Pierce teaches wherein the short term key identifier is calculated by encrypting the short term key identifier and the second random number with the access key (column 4, lines 5-67, column 5, lines 1-25).

Conclusion

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

15. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

17. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136

18. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100